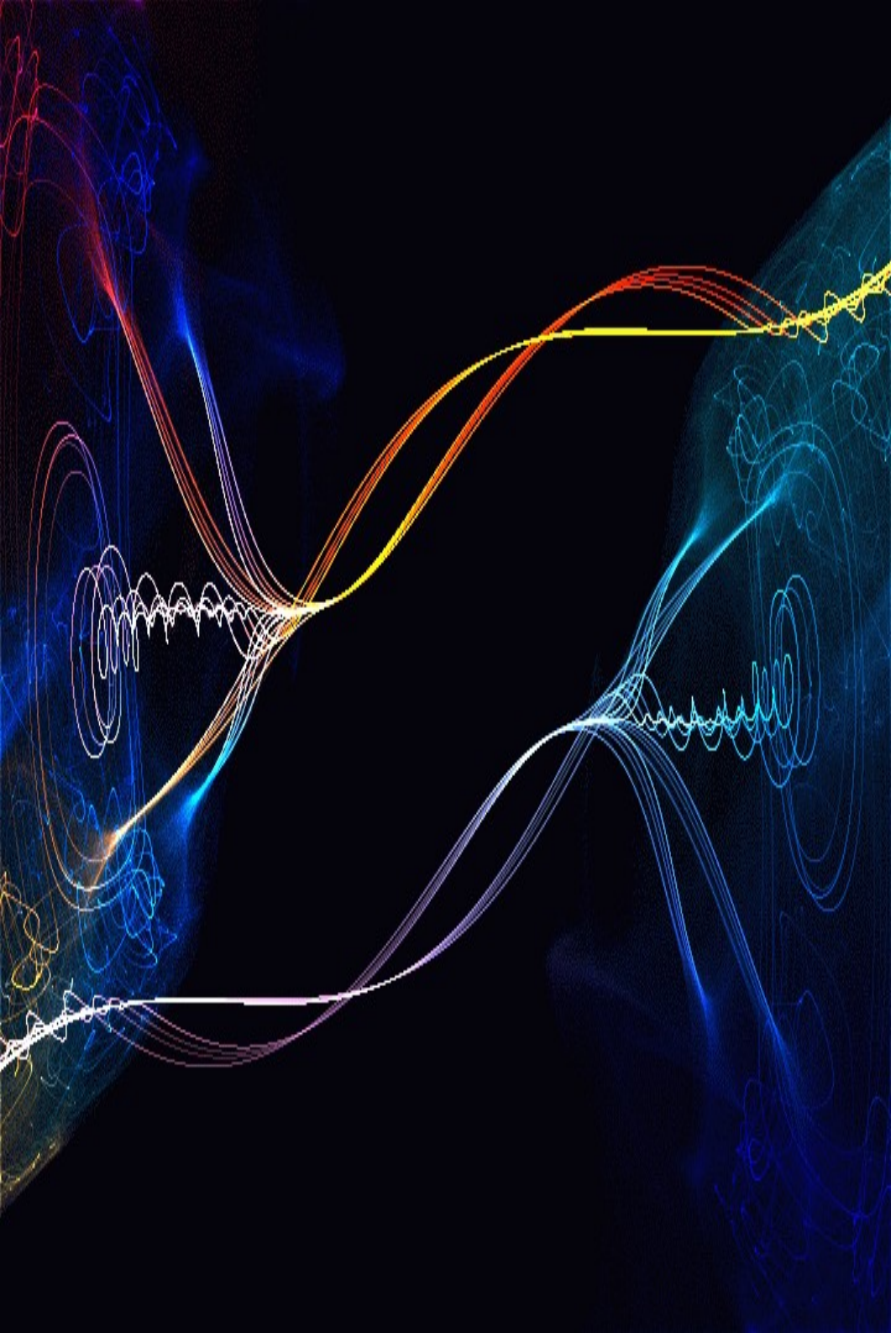


Phishing scam

- Situação atual
- Contramedidas
- Ataques correntes e futuros(?)
- Medidas paleativas
- Cenários futuros
- Conclusões

Nelson Murilo
<nelson@pangeia.com.br>

- Clonagem de páginas
- Redirecionamento de DNS
- *Keylogger*
- *ScreenLogger*
- Cavalos de Tróia com comportamento de vírus (exploração de falhas e/ou arquivos compartilhados)

- Uso de HTTPS na página principal
- Divisão da autenticação em dois passos, com ou sem exibição de informações de cadastro
- Exibição de informações cadastrais logo após identificação
- Autenticação adicional no momento de efetuar a transação financeira

- Robôs para consulta de servidores DNS
- Instalação de programa nos clientes
- As mesmas utilizadas contra clonagem de páginas

- Teclado Virtual
- Botões com duas ou mais letras/números
- Uso de certificados digitais

nelson@pangeia.com.br

- Botões com duas ou mais letras/números
- Certificados digitais
- Instalação de programa nos clientes
- Cadastro de usuários/equipamentos
- Senhas dinâmicas (cartão de segurança)
- OTP (One Time Password)

- Furto de certificado digital
- Retirada de uso do navegador e simulação de seu comportamento
- Uso remoto do computador da vítima, após captura das credênciais
- **Carona em uma conexão autenticada**

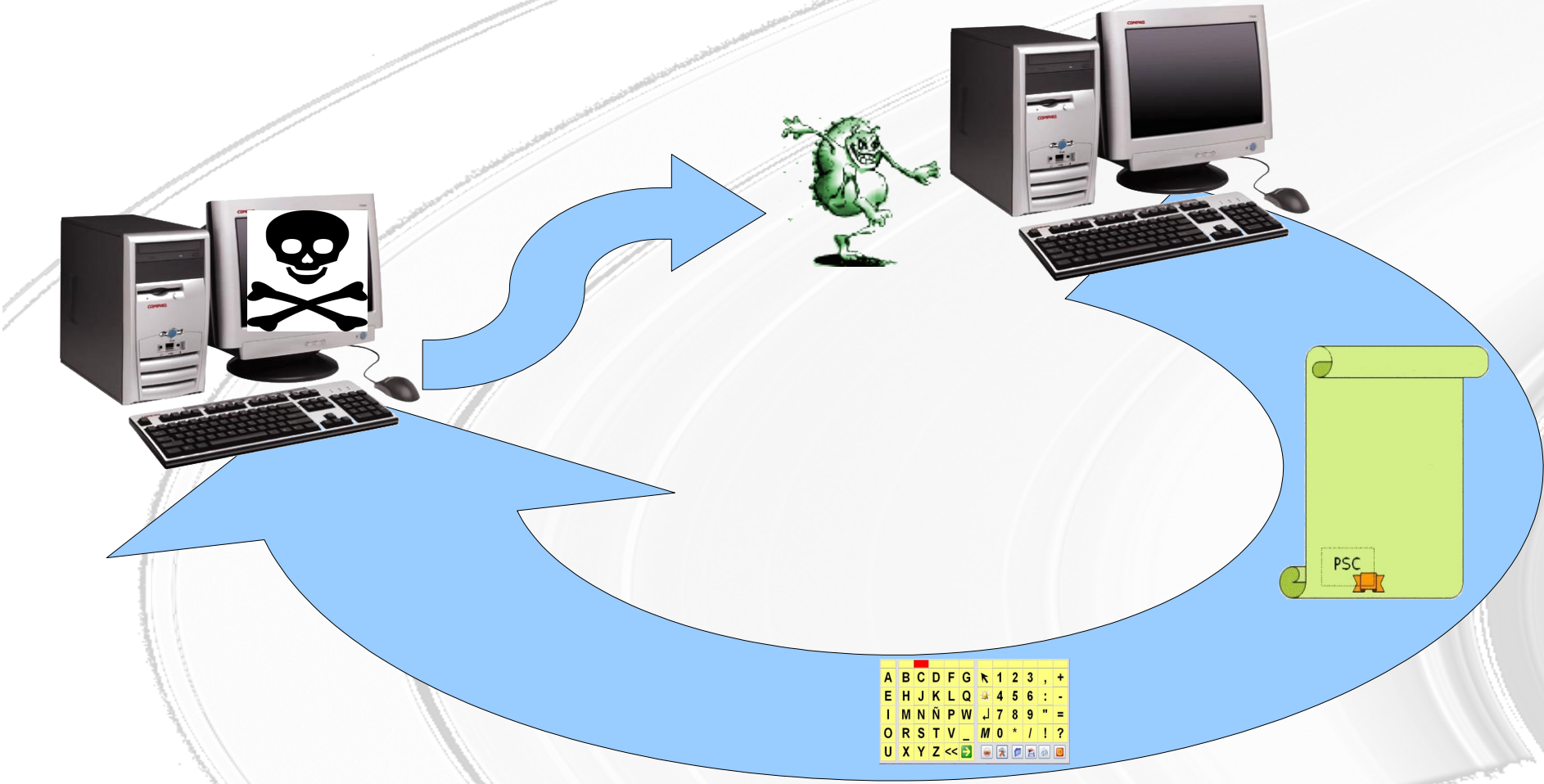
Solução:

Distribuição de cartões com tabelas de números impressos

Problemas:

Não resolve problema de carona em conexão estabelecida. Vulnerável à coleta dos números pelo trojan, após uma certa quantidade de conexões

Soft certificates

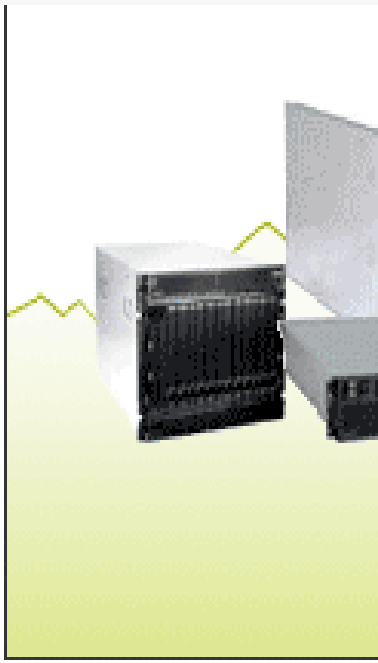


nelson@pangeia.com.br

http://www.cio-today.com/story.xhtml?story_id=13100003EAJT&page=2

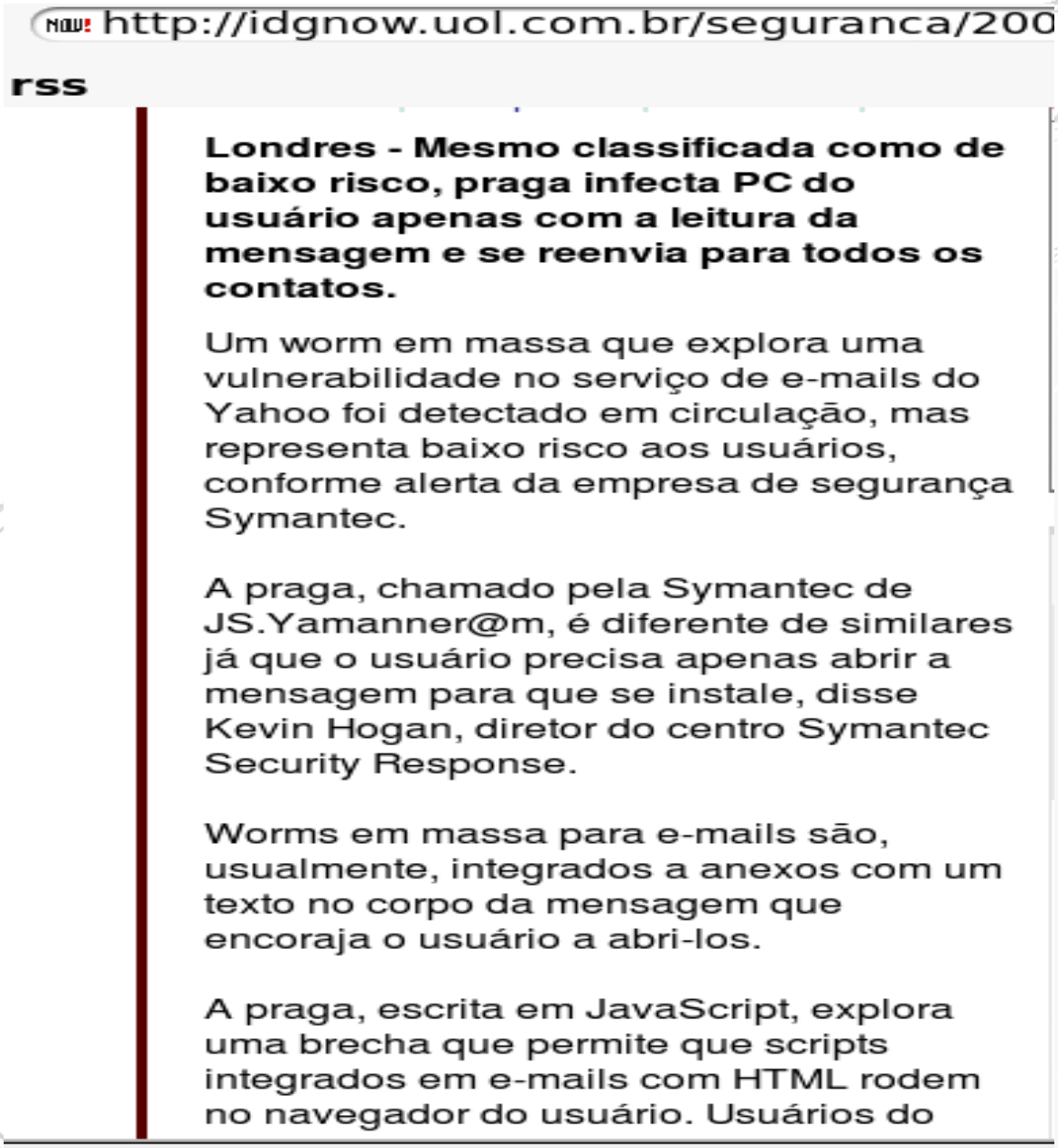
"The problem is," according to one bank regulatory security auditor, "SSL isn't broken. SSL states that the connection between your PC's network card and the bank's network card isn't compromised. This is still true. Nobody is sniffing the transaction off the wire. Instead, this is a 'man-in-the-end-point' attack." In other words, the Trojan is sniffing or manipulating the transaction before it is ever sent across the Internet to the bank.

According to Mitchell Ashley, CTO of network security provider StillSecure, "Traditional phishing attacks have duped end-users into clicking on a link, but in the newest evolution, even the most security-savvy can fall victim to attack. Once you're infected, the game is up."



Network Securi

1. Swedish Police
2. Qwest Offers Q



http://idgnow.uol.com.br/seguranca/200

rss

Londres - Mesmo classificada como de baixo risco, praga infecta PC do usuário apenas com a leitura da mensagem e se reenvia para todos os contatos.

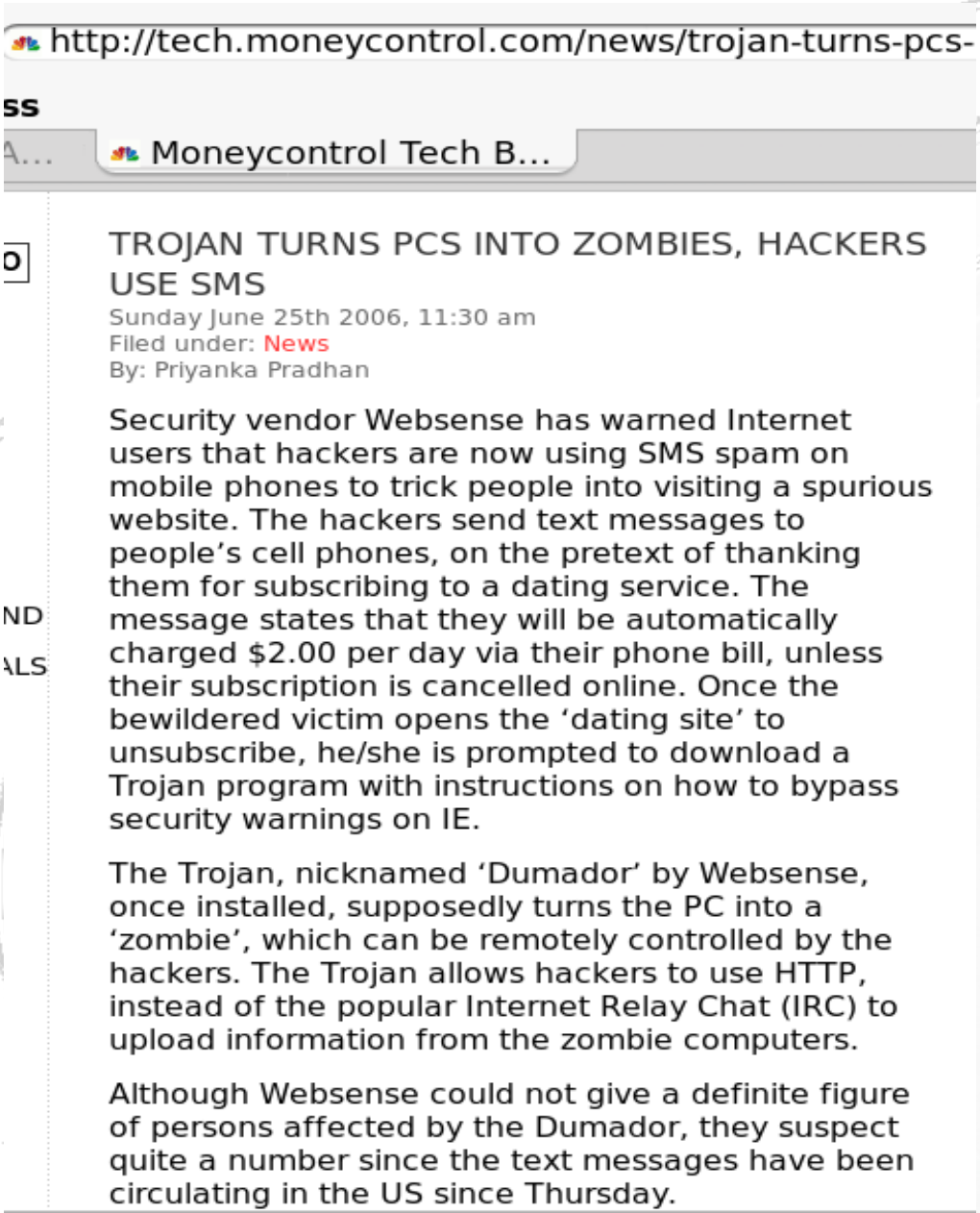
Um worm em massa que explora uma vulnerabilidade no serviço de e-mails do Yahoo foi detectado em circulação, mas representa baixo risco aos usuários, conforme alerta da empresa de segurança Symantec.

A praga, chamado pela Symantec de JS.Yamanner@m, é diferente de similares já que o usuário precisa apenas abrir a mensagem para que se instale, disse Kevin Hogan, diretor do centro Symantec Security Response.

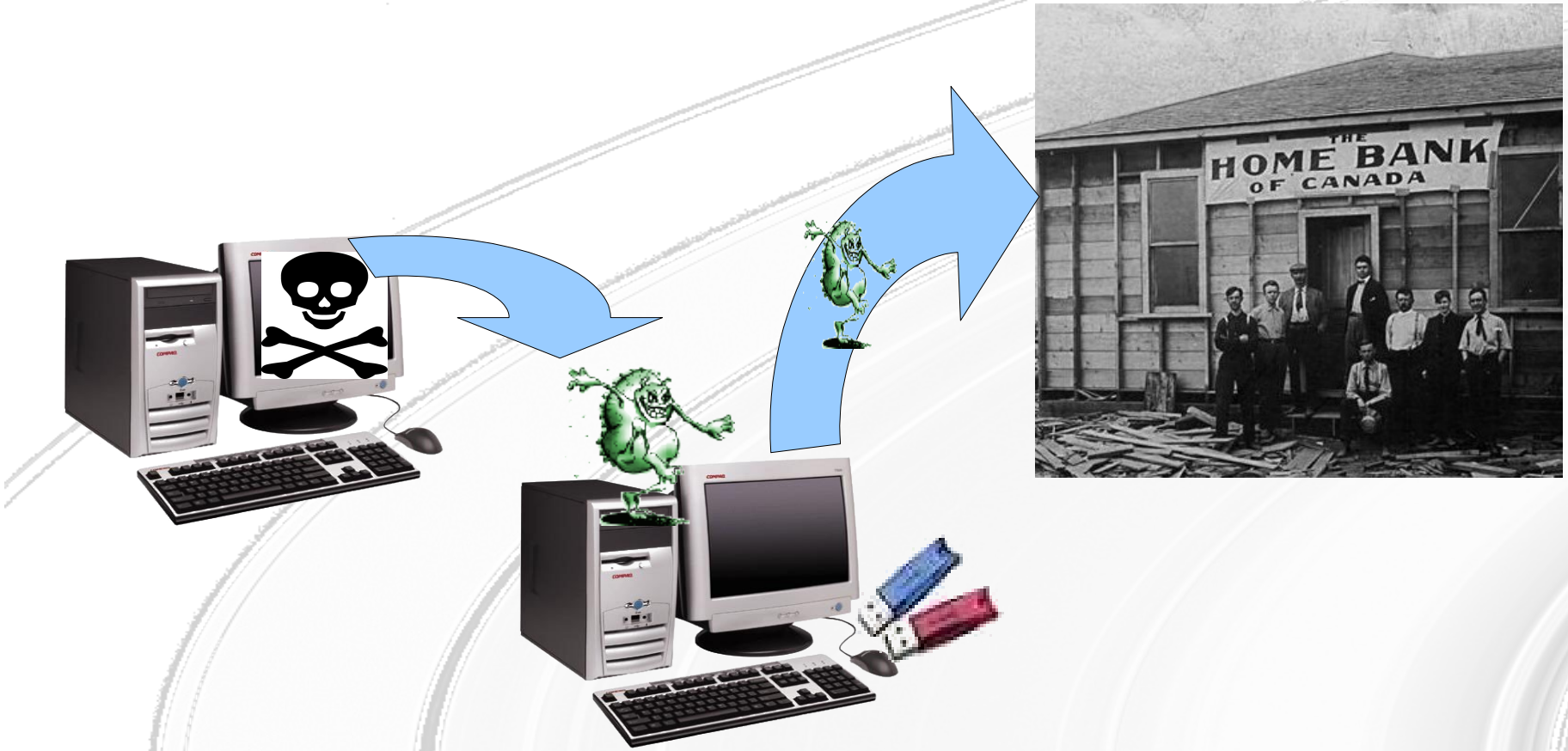
Worms em massa para e-mails são, usualmente, integrados a anexos com um texto no corpo da mensagem que encoraja o usuário a abri-los.

A praga, escrita em JavaScript, explora uma brecha que permite que scripts integrados em e-mails com HTML rodem no navegador do usuário. Usuários do

Fonte: IDGNow
12/06/2006



nelson@pangeia.com.br



- Implementação cara
- Não resolve problema da carona em conexão estabelecida

nelson@pangeia.com.br

- Cadastramento de máquina de cliente
- One Time Password
- Senhas dinâmicas (cartão de segurança)
- Certificação digital
- Biometria

- **Parcialmente mitigado com instalação de programa nos clientes**

nelson@pangeia.com.br

Solução:

Programa trava demais instâncias do navegador, quando acessando o sítio do banco

Problemas:

Limitado a somente um navegador
Navegador falso
Sobreposição do navegador

nelson@pangeia.com.br

Forte tendência de migração das transações do ambiente PC para celular:

- Maior mobilidade
- Fraude zero
- Maior controle aparente do processo

nelson@pangeia.com.br

June 19 2006 at 03:06AM

By Sven Appel

Berlin - Most people forget that cellphones are actually small, portable computers capable of sending and receiving data. Receiving data is good, but it's also possible to receive software that damages the cellphone or its user. In other words: viruses and worms, the bane of the computer world, are now being written for cellphones too.

File Edit View Go Bookmarks Tools Help

http://ipinferno.blogspot.com/2005/10/samsung-wimax-presentation.html

Latest Headl... rss

WEDNESDAY, OCTOBER 26, 2005

SAMSUNG WIMAX PRESENTATION

Hungkwon Song, VP Global Marketing Group, Samsung presented the South Korean perspective on WiMax. Samsung's WiBro technology will be the first mobile broadband technology in the world, and it is being merged into the WiMAX "e" standard.

Korea broadband market:
78% has wireline and wireless data access and next year some uesers will have 100 MB service. There are 37.8 M mobile subscriptions -- 36 M mobile data users. Revenue from data is 25% of ARPU. There are already 12 M EV-DO subscribers. Last year CAGR for the mobile

TELECOM E REDES

MOBILIDADE

Samsung anuncia celular com WiMax para 1º semestre de 2007

Pequim - Executivo da empresa confirmou aparelhos compatíveis com a tecnologia que oferecerá acesso sem fio à web às grandes áreas.

A Samsung planeja para o próximo ano o lançamento de celulares compatíveis com a tecnologia WiMax de acesso à internet. Já no primeiro semestre alguns modelos serão lançados em diversos países do globo.

WIRED WEIGHS IN WITH A NOT VERY THOUGHTFUL PIECE THAT MISUNDERSTANDS CNET

Facilitadores de ataque

- VM Java (j2me) presente na maioria dos celulares atuais
- Mercado **não proprietário** dividido entre:

symbian

Windows Mobile

- Ataque facilitado (wifi/wimax/bluetooth/IPv6)
- Reprodução dos mesmos problemas atuais
  - Redirecionamento de DNS
  - Clonagem de página
  - Key/Screenloggers
  - Carona em conexão estabelecida

- Ataque ao servidor DNS do provedor (Celular com acesso Wi-Fi/WiMax)

- Código malicioso modifica arquivo *hosts*
  - e-mail
  - acesso não autorizado via bluetooth
  - serviço de mensagens instantâneas

SCap.cpp + (/home/nelson/fnt/scap/src) - VIM

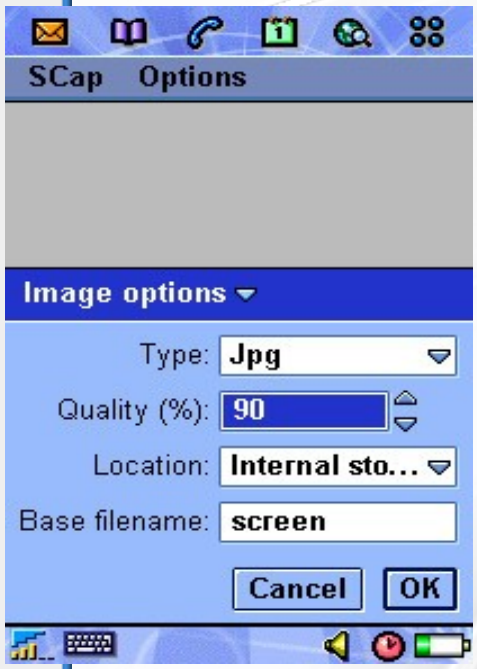
```
void CSCapAppUi::ConstructL()
{
        BaseConstructL();
        iSCapEngine = CSCapEngine::NewL();
        iSCapEngine->SetSaveImageObserver(this);
        iAppView=new(ELeave) CSCapAppView;
        iAppView->ConstructL(ClientRect());

        iWinGroup=RWindowGroup(CEikonEnv::Static()->WsSession());
        User::LeaveIfError(iWinGroup.Construct((TUint32)&iWinGroup));
        iWinGroup.EnableReceiptOfFocus(EFalse);
        iWinGroup.SetOrdinalPosition(0, 1000);
}
void CSCapAppUi::HandleCommandL(TInt aCommand)
{
        switch (aCommand)
        {
                case EEikCmdExit:
                        Exit();
                        break;

                case EEikCmdAbout:
                        DisplayAboutDialogL();
                        break;

                case EEikCmdGeneralOptions:
                        DisplayGeneralOptionsDialogL();
                        break;

                case EEikCmdCaptureStartStop:
                        iSCapEngine->StartStopCapture();
```



nelson@pangeia.com.br

Cenário hipotético

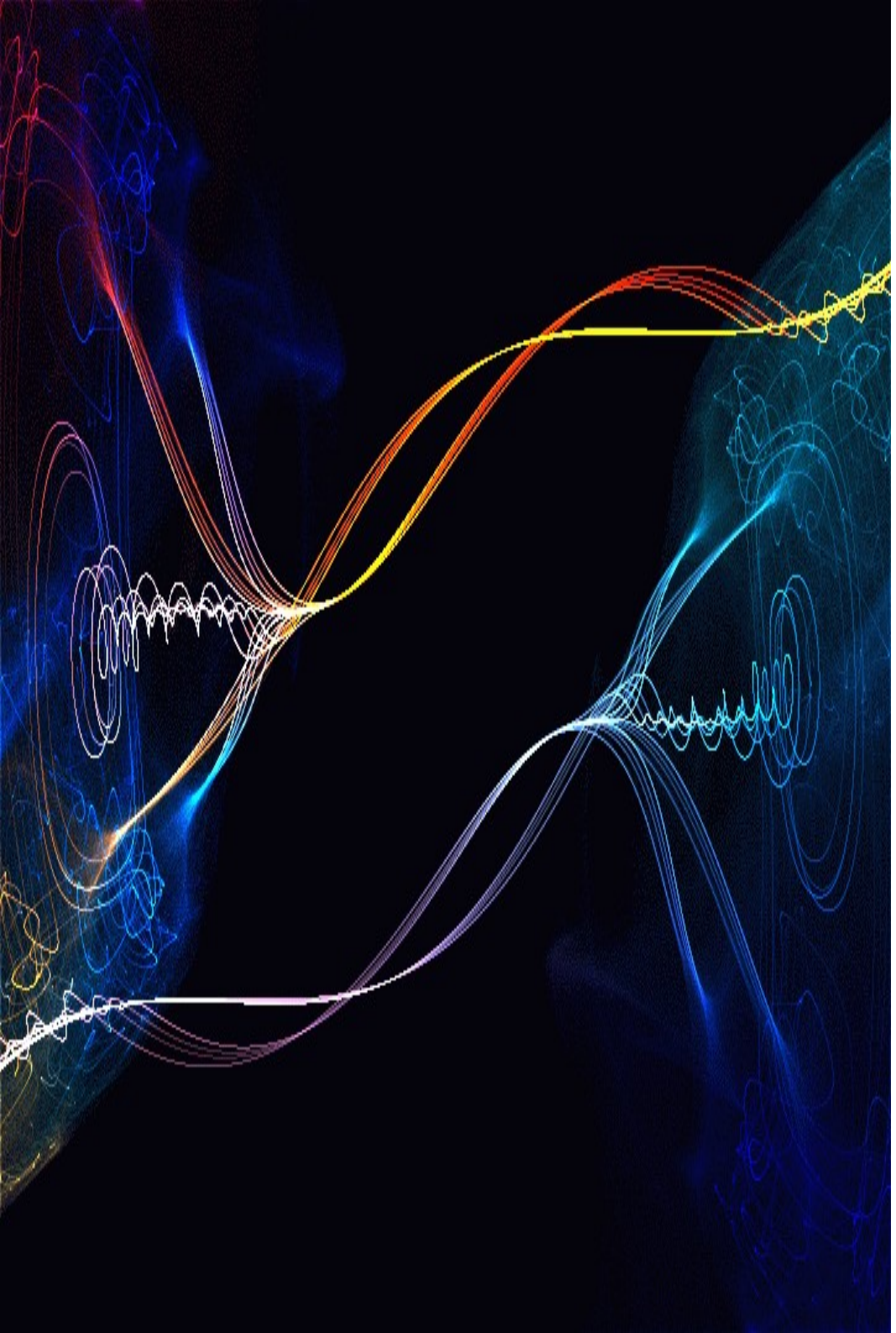
nelson@pangeia.com.br

Cenário hipotético

nelson@pangeia.com.br

Limitadas (navegadores, ambientes, etc.)

- Não cobrem muitos dos problemas já conhecidos
- Não abrangem outros canais e dispositivos
  - URA
  - Celular
- Disseminação do uso via celular deverá abrir novas frentes de ataques



Phishing scam

- Situação atual
- Contramedidas
- Ataques correntes e futuros(?)
- Medidas paleativas
- Problemas
- Soluções

Nelson Murilo
<nelson@pangeia.com.br>